Factorización de enteros con hipérbolas modulares

Expositor: Juan Di Mauro (ICC-UBA, jdimauro@dc.uba.ar)
Autor/es: Juan Di Mauro (ICC-UBA, jdimauro@dc.uba.ar)

El problema de factorización de enteros tiene una gran importancia práctica y teórica. En la práctica, el uso extendido del criptosistema RSA ha estimulado la investigación en algoritmos de factorización eficientes y por eso, el caso que se tratará es $n = pq$ con p, q primos de mangitud $\sqrt{n}$ y $|p - q|$ lo suficientemente grande.

Este trabajo tiene origen en la observación hecha por H. Scolnik, de que para ciertos enteros c la ecuación diofántica $n + x^2 = y^2$ módulo c tiene solución única. Se define como *target* de n a una terna representando la solución. El conjunto de targets guarda una relación estrecha con las hipérbolas modulares y algunas propiedades entre ambos se corresponden directamente.

Por otra parte, las soluciones modulares dan información sobre los factores de n en $\mathbb{Z}$ y pueden ayudar a atacar el problema de factorización. Aunque para casi todos los enteros hay más de una solución, se prueba un resultado de interes en sí mismo: para enteros cumpliendo ciertas condiciones, el cociente entre la cantidad de soluciones módulo c y c tiende asintóticamente a 0. Un nuevo algoritmo de factorización es construido a partir de eso y se estima su tiempo de ejecución. Instancias de prueba de la implementación del algoritmo corroboran el tiempo de ejecución estimado.